Public Comments Regarding Draft FIPS 140-2, Security Requirements for Cryptographic Modules

[in response to a notice in the November 17, 1999 Federal Register
(Volume 64, Number 221; pages 62654-62655)]

X-Mailer: Novell GroupWise 4.1
Date: Mon, 24 Jan 2000 17:09:51 -0500
From: Louis Grosman <LHG@nrc.gov>
To: Proposed140-2@nist.gov
Cc: DHG@nrc.gov, EMP1@nrc.gov, JLC5@nrc.gov
Subject: Review of Draft FIPS 140-2 (OCIO Ticketed Item 00-007)

The NRC has reviewed the Draft and has no comments.

Louis H. Grosman, CISSP
USNRC T6 F15
Washington, DC. 20555
Phone: 301-415-5826
Fax: 301-415-5368
Pager 888-614-1607
E-mail: lhg@nrc.gov
Pager: 1-888-614-1607
Pager Mail: 6141607@skytel.com

From: "Costantini, Frank @ CSE" <fcostant@mail.cse.l-3com.com>
To: "'proposed140-2@nist.gov'" <proposed140-2@nist.gov>
Cc: "Carter, Matthew @ CSE" <matthew.carter@l-3com.com>,
"Kozak, Taras @ CSE" <tkozak@mail.cse.l-3com.com>
Subject: Comment on FIPS-140-2
Date: Wed, 26 Jan 2000 14:26:10 -0500
X-Mailer: Internet Mail Service (5.5.2650.21)

FIPS-140-2 Group:

After reviewing the draft of FIPS-140-2, I believe that the following section regarding self test (section 4.9) needs to be modified to address the needs of secure telephony devices:

"When a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status interface. The cryptographic module shall not perform any cryptographic operations while in the error state and no data shall be output via the data output interface while the error condition exists."

Secure telephony devices and security appliques to existing telephones spend most of their time in a non-secure state, with the user only rarely requiring secure operation. If the cryptography function of a secure telephony device fails, the user would still expect the device to be able to make nonsecure calls. In fact, other federal regulations would require that the phone still be able to make emergency calls. The current wording of the proposed standard would not allow this to occur. I think the paragraph should read as follows:

"When a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status interface. The cryptographic module shall not perform any cryptographic operations while in the error state. Bypass operation shall be permitted provided that the error indication is available to the user and provided that the user is given an indication that the bypass function is active. Otherwise, no data shall be output via the data output interface while the error condition exists."

Likewise, Section 4.2 should allow bypass operation in the absence of operating power without "two independent" operations. Telephones are supposed to operate during a power failure. The focus should be on user expectations: as long as the product never provides a bypass operation when the user would expect a secure connection, then the product should satisfy the criteria.

Thank you for your consideration. If you would like to discuss this further, please feel free to contact me.

Regards,

Frank Costantini

L-3 Communications
Communication Systems-East
1 Federal Street, AE-3C, Camden, NJ 08103
*856-338-3480   Fax: 856-338-3150
email: frank.costantini@L-3COM.com

Reply-To: <fbi09@earthlink.net>
From: "Harry Reves" <revesh@fbiacademy.edu>
To: <proposed140-2@nist.gov>
Cc: "Jim Downes" <James.Downes@cio.treas.gov>,
"Dwight Locke" <dwight.locke@cio.treas.gov>,
"Kyle Sinclair" <kyle.sinclair@cio.treas.gov>,
"Jim Foti" <jfoti@nist.gov>
Subject: OTAR
Date: Fri, 4 Feb 2000 10:50:56 -0500
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook 8.5, Build 4.71.2173.0
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.2106.4

Sir, In reviewing the proposed FIPS 140-2 document I have noted a over sight in the area of Cryptographic Key Management section 4.7 of the document. Being a user of the standards for the Federal Bureau of Investigation, we have requirements in the wireless communications systems we deploy for Over The Air Rekeying (OTAR) of the subscriber devices. There is no reference in this section of the document to address wireless rekeying of the subscriber devices. It appears that the only areas that are addressed are the manual connection of a key fill device or a wireline connection for key fill. Being a user of RF or wireless equipment and having to use these standards for our operational need this is a requirement that needs to be addressed in the standard.

Harrison Reves
Telecommunications Manager
Federal Bureau of Investigation
FBI ERF
Building 27958A
Quantico,VA 22135

Phone (703) 632-6712

From: "Epstein, Sandy" <Sandy.Epstein@racalns.com>
To: "'Proposed140-2@nist.gov'" <Proposed140-2@nist.gov>
Cc: "Ricketts, Andrew" <Andrew.Ricketts@racalitsec.com>,
"Davies, Peter"
<Peter.Davies@racalns.com>,
"Woods, Chris" <Chris.Woods@racalitsec.com>,
"Evans, Nicky" <Nicky.Evans@racalitsec.com>,
"Lomax, Chris"
<Chris.Lomax@racalitsec.com>,
"Carter, Ron" <Ron.Carter@racalitsec.com>
Subject: Comments on Draft FIPS 140-2
Date: Mon, 14 Feb 2000 16:33:07 -0500
X-Mailer: Internet Mail Service (5.5.2448.0)

[Comments attached.]

Comments on Draft FIPS 140-2

Racal Security and Payments submits the following comments and recommendations regarding Draft FIPS Pub 140-2 in response to the Federal Register notice, Volume 64, No. 221, dated Wednesday, November 17, 1999.

1. General

Racal believes that Draft FIPS 140-2 is a general improvement on FIPS 140-1. However, we also feel that there are areas of ambiguity and areas where more detail is required.

2. Comments that Apply Across the Document

2.1 Choice of Algorithm

As in FIPS 140-1, the draft insists on the use of cryptographic algorithms referenced in a Federal Information Processing Standard. This is not an issue for obvious algorithm requirements such as encryption, but can cause problems for less well-defined requirements such as random number generators, etc., where bureaucracy can end up overriding good practice. Perhaps it should be made clear for which requirements FIPS specified algorithms apply.

3. Comments that Apply to Particular Paragraphs

3.1 Section 14 of the Announcement on Implementation Schedule

This section states that all products currently accredited to FIPS 140-1 will lose their approval 12 months after publication of FIPS 140-2 and not be available to Federal agencies for new purchases. There are both practical and theoretical problems in this approach.

The practical issue is that all 87 evaluated products must be re-evaluated during the 12-month transition period if they are to remain available to end users. Given the implied workload, it may not be possible to do so. If it is not possible, which vendors should suffer by losing their ability to sell products because of a lack of capacity to perform the evaluations? This problem may be further compounded by the addition of new types of evaluations such as those against the Common Criteria, which may be burdensome and for which the evaluation process is less mature. During this transition period, if all existing products must be re-evaluated, what impact will that have on the evaluation of new products?

From another point of view, a short transition period like the one proposed would seem to imply that there are material defects or shortcomings in FIPS 140-1 that require the products to be changed and re-evaluated quickly. We do not believe that to be the case; FIPS 140-2 is an incremental improvement on FIPS 140-1. The changes between FIPS 140-1 and FIPS 140-2 are significant but not that extensive. Some modules evaluated against FIPS 140-1 may require little if any change nor added testing to meet FIPS 140-2.

In addition the transition plan is a disincentive to vendors to submit further products to FIPS 140-1 evaluation, since the vendor must incur the cost to re-evaluate the product against FIPS 140-2 before the vendor can recapture the cost of the initial evaluation through sales of the product.

We therefore suggest that the public interest may be better served by preventing evaluations against FIPS 140-1 from commencing as of the date of publication of FIPS 140-2 and (a) extending the transition period for products certified under FIPS 140-1 to 2 years after the publication of FIPS 140-2, or (b) NIST identifying and grandfathering those FIPS 140-1 approved products which because of their properties (as presented in the FIPS 140-1 laboratory report) meet FIPS 140-2 without modification or re-evaluation, or (c) NIST specifying the requirements imposed by FIPS 140-2 that are in addition to those of FIPS 140-1 and require evaluation for modules approved to FIPS 140-1 and requiring that FIPS 140-1 compliant products be evaluated within two years during which period the product is granted temporary approval as FIPS 140-2 compliant.

3.2 Para 3 Functional Security Objectives

We recommend that the third bullet be modified to add “algorithms” to the list of critical components that require protection against unauthorized and undetected modification. This is relevant both to hardware implementations that allow for soft loaded algorithms and for software implementations.

3.3 Para 4.2 Requirement on the Production of Status Information is Restrictive

Any cryptographic module is required to produce status information indicating its current operational state. This is intended to take the form of a "status output interface". This is a little restrictive, and although the criteria allow for other styles of indication, these are not clearly defined.

We suggest that the criteria should clarify the other styles of indication allowed, and that these should not be unduly restrictive.

3.4 Para 4.7 Choice of Key Management Techniques

There is an intention voiced in the criteria to move to a requirement for FIPS approved key management techniques. Currently, commercially available techniques are permitted for this purpose, and it would be worth insisting that this remains the case.

We recommend that commercially available key management techniques should continue to be permitted.

3.5 Para. 4.7.2 Key Generation

The draft requires that intermediate key values shall not be accessible in *' … plaintext or otherwise unprotected form'*. The term 'unprotected' is a little vague here.

We suggest that the term 'unprotected' should be clarified. Perhaps a definition of suitable protection would assist the reader.

3.6 Para 4.7.5 Key Storage

The draft talks about the storage of secret and private keys and the requirement to either encrypt these keys or store them in plaintext. In the next sentence it talks generally about plaintext keys not being accessible from outside the cryptographic module. The draft needs to state that it is only these secret and / or private plaintext keys that are being referred to here.

3.7 Para 4.5, 4.7.6 Key Destruction

The draft in several places requires the capability to zeroize keys. In many case it is not specified how fast this is to be done, in other cases the word 'immediately' is used. This seems a little too open to interpretation. Implementations can be imagined that perform this function in times ranging from nanoseconds to minutes.

We suggest that further clarification is given here and that where zeroizing is required 'immediately' then a maximum time should be specified.

3.8 Para 4.9.2 Testing and Notification of Plaintext-Bypass Modes

The standard includes a significant set of requirements with respect to testing and user notification of plaintext-bypass modes. However the bypass test is not well defined.

We suggest that the bypass test be clarified further.

3.9 Appendix C - Cryptographic Module Security Policy

The definitions and requirements of the Cryptographic Module Security Policy seem to lack detail. Example documents to accompany the criteria would assist here.

We recommend that an example Cryptographic Module Security Policy be provided to help readers understand the level of detail required here.

X-Sender: frousseau@adga.ca
X-Mailer: Windows Eudora Pro Version 3.0.1 (32)
Vipers11
Date: Tue, 15 Feb 2000 11:14:59 -0500
To: Proposed140-2@nist.gov
From: Francois Rousseau <f.rousseau@adga.ca>
Subject: Comments on Draft FIPS 140-2

Here are two minor comments on the Draft FIPS 140-2 document:

a. For the functional requirements of operating systems, the document refers to a superceded version of the Common Criteria (CC) Controlled Access Protection Profile (CCAP) instead of the officially registered version (i.e. version 1.c, January 29, 1999 instead of version 1.d, October 8, 1999); and

b. Paragraph 1.2, for a FIPS 140-1 Security Level 2 the document only mandates that operating systems be evaluated at the CC evaluation assurance level of EAL2 although the assurance level mandated in the CCAP is of EAL3.

François Rousseau
Senior IT Security Consultant
AEPOS Technologies Corporation
200 Montcalm, Suite 200
Hull, Quebec, J8Y 3B5

mailto:f.rousseau@adga.ca Tel: (819) 772-8522 Ext 314
http://www.aepos.com Fax: (819) 772-0449

Server Systems Development

Cryptographic Hardware Technology Development
MS P371, 522 South Road, Poughkeepsie, NY 12601

February 11, 2000

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Subject: FIPS 140-2 Comments

Attached are comments related to the public feedback in regard to the new FIPS 140-2 Standard, Security Requirements for Cryptographic Modules.

Sincerely,

Randall J. Easter
Senior Engineer, Cryptographic Hardware Technology Development
reaster@us.ibm.com
Tel: (914) 435-8313
Fax: (914) 435-1858

Enclosures:

cc:

Section 4.9 Self-Tests

This section discusses the need for self-tests to ensure that a module is functioning properly. The idea is that whenever a module is powered up (i.e., Power-Up tests) these tests are performed.

Modules that are designed to be used in high availability environments that require nonstop 24x7 operation may only perform power-ON's very infrequently or even only once during initial installation. The example is a Server environment that utilizes a cryptographic module, which is very different than a client PC environment where power-ON's may be frequent. In this environment a one-time power-on test gives no assurance that over time the module continues to operate properly. A simple known-answer test also does not guarantee adequate test coverage of the modules algorithmic functions as it may not check the majority of the circuits that would be used in normal operation. In addition, there are implementations that are purely hardware that do not have a adjunct processor within the secure Crypto module boundary to assist in performing these self-tests.

An alternate solution that can provide a more robust and continuous checking of the proper functioning of the Crypto module should be allowable. For hardware only implementations, there are well know state-of-the-art techniques of Error Detection and Fault Isolation (ED/FI). ED/FI techniques not only can provide broader assurance coverage of the algorithmic functions, but also the surrounding functional logic. In addition, this checking is typically continuous both during idle periods and during the actual execution of cryptographic operations. In regard to hardware implementations, as technology advances, the integration of Crypto modules in even smaller packages, such as single-chip implementations, will become the norm, rather than multi-chip implementations. For these types of implementations, ED/FI techniques to ensure proper operation will become standard.

Therefore to restate: the requirement for a mechanism to “ensure that the module is functioning properly” should not only allow power-on tests such as a simple known-answer testsas described, but should provide as an alternative, ED/FI techniques as well.

4.9.1 Power-Up Tests

Statistical Random Number Generator Tests

The requirement for this tests implies that a Crypto module *must* include a programmable microprocessor to allow the implementation of the complex RNG tests. However, a single chip hardware only implementation of algorithmic engines that would also include a PRNG or RNG may not have the ability to include these complex tests.

In lieu of the requirement of the Crypto module to internally perform these tests, it should be acceptable for the Crypto module to supply the requisite set of 20,000 consecutive bits of output and have the tests performed by an external adjunct processor.

CYGNACOM SOLUTIONS

February 15, 2000

Dear Sir:

CygnaCom Solutions appreciates the opportunity to comment on FIPS 140-2: Security Requirements for Cryptographic Modules Version 4.4.1. As one of the four laboratories accredited under the National Voluntary Accreditation Program (NVLAP) to test vendor products for conformance to FIPS 140-1 and as a TTAP Common Criteria testing laboratory, we have had a great deal of experience with the testing of security products. In our view the FIPS 140-1 testing has been highly successful because it has established a reasonable balance between the specification of effective security requirements and the resources needed to verify that the requirements have been fully met. No testing program can guarantee security, yet many programs have failed because, in striving for perfect security, they have become an unacceptable burden in terms of required resources (both time and money).

For this reason, we recommend that NIST further revise Draft FIPS 140-2 before proceeding with its approval as a standard. Our main concern is that Section 4.10 Design Assurance requires twenty-two documents and an unspecified number of undefined functional tests. Many testing programs involve every document and every test that the program developers can envision. Some are even open-ended requiring that the product vendor devise tests that were not envisioned by the program developers. On the other hand, FIPS 140-1 Cryptographic Module Validation Program was successful because it limited itself to only those documents and tests that were actually needed. Much of Section 4.10 is inconsistent with this laudable goal. We believe that not only will the increased costs make the program less successful, but also several of the new requirements will add little to the security of validated products. Our specific comments are enclosed. Thank you for considering our views.

Sincerely,

Edward Morris
CEAL Manager

Specific Comments

1. (Section 4.3.3, Operator Authentication) We recommend that for each attempt to use the authentication mechanism, the probability shall be less than or equal to one in 1,000,000 that a random attempt will succeed. This would allow a six-digit password system.
2. (Section 4.5.3 and Section 4.5.4) Multi-Chip Embedded and Multi-Chip Standalone modules with removable covers should provide for automatic key zeroization at Levels 3 and 4. This provision seems to have been inadvertently removed. (See FIPS 140-1).
3. (Section 4.6 Level 2 audit requirements) Common Criteria terms such as "security attributes", "objects", and "rights" are used but not defined. If FIPS 140-2 is intended to be a stand-alone document, then they should be defined.
4. (Section 4.6, Level 2, audit trail modification) While it will be necessary to delete an audit trail in order to live within module memory constraints, it is not clear that there ever is a legitimate reason for modifying the audit trail. If so, then this event need not be audited.
5. (Section 4.6 Level 2 audit requirements) Requiring a Level 2 device to be capable of auditing twenty-three events seems excessive. We recommend that fewer than ten events should be audited for Level 2 and fewer than twenty events should be audited for Level 3. Some events that should be considered for exclusion are: "all requests to perform an operation on an object covered by the security policy;" "any use of an authentication mechanism (e.g., login);" "all attempts to use the user identification mechanism, including the user identity provided;" and "execution of the tests of the underlying machine and the results of tests." Only failed tests need to be audited.
6. (Section 4.7.1, Random and Pseudorandom Number Generators) It would be useful if NIST would specify some optional offline tests that vendors might use to test their random number generators.
7. (Section 4.7.4 Key Entry and Output) This section has been revised so that it is no longer clear that manually distributed secret and private keys can be output in plaintext form. This point should be clarified.
8. (Section 4.10 Design Assurance, general remark) This section appears to be an attempt to level assurance requirements taken from the Common Criteria. Unfortunately, this section is inconsistent with the goals of FIPS 140-1 and the other sections of Draft FIPS 140-2 that make specific requirements on the device itself. Rather than specifying what is required, Section 4.10 requires documentation. Documentation requirements, by themselves, are not a cost-effective means of improving the security of products.
9. (Section 4.10) This section contains twenty-two documentation requirements. In many cases it is not clear what is the underlying product requirement (if any), who is the intended reader of the document (e.g., the vendor, the cryptographic module user, the testing laboratory, or some evaluator of the system), and how the document is to be used. This information might appear in a Device Test Requirements document. However, some of the documentation may be found to be unnecessary when the purpose, user, and the use of the documentation are fully explained.
10. (Section 4.10.1 Configuration Management, Security Level 1, first bullet) It is not clear whether each copy of a configuration item must have a unique number or each type of

configuration item must have a unique number. For an operating system, is the model and version number sufficient or must the serial number be listed as well?

11. (Section 4.10.1 Security Levels 2,3, and 4, third bullet) How does this requirement differ from that of Security Level 1, bullets 1-2?
12. (Section 4.10.2 Security Levels 2, 3, and 4, bullet 1, last sentence) Many commercial products will be shipped through the U.S. mail and sold through authorized dealers. Others might be electronically downloaded to a user's computer. It is not clear whether these distribution methods are adequate for Levels 2-4. This brings up a major problem with Section 4.10. Rather than specifying what is required, this section often just requires documentation of what is done. The Common Criteria accreditation process provides for both the specification of certain types of delivery documentation and the evaluation of the provided documentation. This process differs from the Cryptographic Module Validation program where a major evaluation of the product is not currently required.
13. (Section 4.10.5 Functional Testing and Test Coverage) This section should be eliminated. The FIPS 140-1 Device Test Requirements (DTR) already specify many functional tests. If additional tests are required, then NIST should specify them in the DTR.

From: Marc Laroche <marc.laroche@entrust.com>
To: Proposed140-2@nist.gov
Subject: Comments on the proposed FIPS 140-2 standard
Date: Tue, 15 Feb 2000 15:22:49 -0500
Importance: high
X-Mailer: Internet Mail Service (5.5.2650.21)

Sir/Madam,

This message is in response to your request for comments on the proposed FIPS 140-2 standard. The following comments and recommendations are hereby submitted by Entrust Technologies:

1) Overall rating
Differentiating cryptographic modules using an "overall rating" does not seem appropriate. Considering that the most significant differences between the overall validation levels have to do with Physical Security and Operating System Security. The current "overall rating" system does not adequately reflect the security strength of cryptographic modules. For example, a software cryptographic module with Roles/Services, Key Management and Self-Test at Level 3 with all other levels at level 1 (thus with an overall Level 1 rating), could actually provide higher security and assurance when operated in a secure environment than another cryptographic module that would be validated to Level 2 in all FIPS 140-2 categories. We believe that the current "overall rating" system can be misleading in providing customers with a sense of security that cannot always be justified.

Recommendation: Replace the "overall rating" system with a "two rating" system composed of:
a) an environmental protection rating (physical security and OS Security);
b) a crypto strength rating (other requirements + assurance).
(assurance could also have its own rating).

The main benefit of this approach is to independently reflect the cryptographic qualities of a module versus the environmental protection it provides. This way customers would have a better appreciation of the ratings. Customers could also define requirements for FIPS 140-2 validated modules that would fit better within their operational environments. Another benefit is to allow the cryptographic quality of all module types (e.g. hardware, software and firmware) to be compared equally.

2) Module interfaces
FIPS 140-2 Section 4.2 states "For security Levels 3 and 4, the data input and output physical port(s) used for ... shall be physically separated from all other ports of the cryptographic module." Since this requirement is specific to physical ports, we assume that it does not apply to logical interfaces of software cryptographic modules. Consequently, a software cryptographic module would not need to comply with this requirement and it would be possible for a software cryptographic module to obtain a Level 3 or 4 for Module Interfaces.

Recommendation: The Module Interfaces requirements should be written in such a way that it is possible for software and firmware modules to obtain a Level 3 or 4 for Module Interfaces. In fact, this should be extended to all classes of requirements as it should be possible for a software cryptographic module to attain a Level 3 and 4 (except of course for Physical Security).

3) Enforcement of Roles at Level 1
FIPS 140-2 Section 4.3 states that a cryptographic module shall support a User Role and a Crypto Officer Role. It also mentions that multiple roles may be assumed by a single operator. Since multiple roles can be assumed by a single operator and considering that authentication is only optional for level 1, the requirement for supporting roles at Level 1 is not deemed to be appropriate.

Recommendation: As a minimum, authentication in a Crypto Officer Role should be enforced at Level 1 or, there should be no requirements to support roles at Level 1.

4) Non-FIPS approved modes of operation
FIPS 140-2 Section 4.1 states: "A cryptographic module shall implement at least one Approved algorithm or Approved security function used in an Approved mode of operation. Other algorithms or security functions may also be included for use in non-Approved modes of operation. The operator shall be able to determine when an Approved mode of operation is selected."

Recommendation: It should be made possible to enforce this requirement simply by including appropriate statements in the security policy, assuming that cryptographic module operators have the capability to specify the cryptographic algorithm and function to run.

5) Role-based Authentication
FIPS 140-2 Section 4.3.3 states: "The cryptographic module shall require that the operator select one or more roles ...", which looks very rigid in comparison to FIPS 140-1 which allows the operator to implicitly select one or more roles. In many cases (actually in a majority of applications), operators do not explicitly request cryptographic services. The cryptographic services are often hidden to users and are implicitely invoked by applications initiated by users. The requirement for explicit selection of a role would make it very cumbersome to users. To be effective, cryptographic services must be transparent to users as much as possible, or some users may decide to avoid using them ...

Recommendation: This requirement should be stated as in FIPS 140-1, i.e. "The cryptographic module shall require that the operator either implicitly or explicitly select one or more roles ..."

6) Operating System Security: Interpretative language

FIPS 140-2 Section 4.6 (Security Level 1) states that "All cryptographic software shall be installed as executable code in order to discourage scrutiny and modification by users." This implies that cryptographic module built using an interpretative language such as JAVA would not satisfy the Operating System Security requirements. (Is this really a OS Security requirement?)

Recommendation: Interpretation and guidance statements should be provided to address the issue of software cryptographic modules that are written using an interpretative language. FIPS 140-2 must address the trust model required for an interpretative language such as JAVA.

7) Operating System Security: Audit Requirements

FIPS 140-2 Section 4.6 defines Audit requirements for security levels 2 and above.

a) Because these requirements must be satisfied by the Operating System and not the cryptographic module, they should be defined in the CAPP, not in the FIPS 140-2 standard. The Operating System vendors are in a much better position to demonstrate conformity with these Operating System specific requirements than cryptographic module vendors. For example, security attributes must be clearly defined in a Protection Profile or Security Target as they may vary from product to product.

b) Some of the defined audit requirements correspond to Operating System events and others to software cryptographic events. As mentioned in a), the audit requirements that apply to the Operating System should not be defined in FIPS 140-2 but instead they should be included in the CAPP, and audit requirements that relate to software cryptographic modules should be implementation independent, i.e. they should apply to any type of modules including software, hardware and firmware. Consequently, these requirements should be grouped in a new class called Audit.

c) Some of the Audit requirements are practically speaking not achievable. For example, a role defined for a module is likely to be transparent to the OS. If the module is an executable, then the OS will only see an application that starts and ends; the OS will not even see the login to the application. If the module is a static library embedded within an application, then the OS doesn't see the module; the module interface is hidden and can't be seen outside of the application. In this case, cryptographic module activity cannot be audited by the OS since the Operating System audit function has no way of seeing what takes place at the cryptographic level.

d) In the case where a cryptographic module is embedded within a trusted application and where the module cannot be accessed from outside of the application, the OS access control requirements become irrelevant. Consequently, it should be possible for a cryptographic module that is embedded within a CC EAL2 (or EAL 3 or EAL4) evaluated application to be granted a Level 2 (or Level 3 or Level 4 respectively) rating for OS Security, given that the trusted application provides access control and a security assurance that is equivalent to the CAPP (EAL2, EAL3 or EAL4).

Recommendations:
a) Operating System Audit requirements should be included in the CAPP and not in FIPS 140-2.
b) Cryptographic module requirements for Audit should apply to all types of modules including software, hardware and firmware modules (not only to software modules).
c) The Audit requirements should be revisited in light of the comments stated above in 7a, 7b and 7c.
d) Section 4.6 Security Level 2, Security Level 3 and Security Level 4 should allow for trusted applications to be treated as equivalent to trusted OS in cases where a cryptographic module is embedded within a trusted application and cannot be accessed from outside of the application.

8) Key Distribution
Section 4.8.2 of FIPS 140-1 "Key Distribution" has been replaced by section 4.7.3 "Key Exchange/Agreement" in FIPS 140-2. However, key distribution is still mentioned in FIPS 140-2 (e.g. electronically/manually distributed keys) but a clear definition for "key distribution" is not provided.

Recommendation: A clear definition for "Key Distribution" should be provided.

9) Key Storage

Section 4.7.5 of FIPS 140-2 states: "When contained within a cryptographic module, secret and private keys shall be stored in plain text form or shall be encrypted using an Approved algorithm." This requirement seems odd. Basically, it means that keys may be stored in plain text, but what if keys are encrypted using a non-Approved algorithm, or obfuscated using a proprietary technique?

Recommendation: Given that the storage of keys in plain text is allowed, storage of keys using a non-Approved algorithm should also be allowed.

10) Delivery and Operation

Section 4.10.2 Security Level 2, 3 and 4 of FIPS 140-2 states: " ... This shall include how the integrity of the hardware and software are protected from modification and substitution." This requirement ("protection from modification and substitution") is similar to the Common Criteria ADO_DEL.3 requirement which is not mandated for CC assurance levels lower that EAL7. This requirement seems too high in this context.

Recommendation: This requirement should be modified to be equivalent to ADO_DEL.2 ("detection of modification and substitution") which is deemed to be more appropriate.

11) Guidance Documents

Section 4.10.4 of FIPS 140-2 defines requirements for Administrator Guidance. In cases where the cryptographic module is not a commercial product but a component that can be embedded into products, guidance documents are likely not to exist.

Recommendation: When the cryptographic module is not a commercial product, Programmer's Guide and Security Policy documents should be allowed to be provided as guidance documents.

Sincerely,

Marc Laroche
Manager Product Evaluation
Entrust Technologies

From: sws@us.ibm.com
X-Lotus-FromDomain: IBMUS
To: proposed140-2@nist.gov
Date: Tue, 15 Feb 2000 16:11:58 -0500
Subject: comments

(See attached file: draft.pdf)

[Comments attached.]

Comments on FIPS 140-2 Draft

Secure Systems and Smart Cards
IBM T.J. Watson Research Center
S.W. Smith, editor

February 15, 2000

Background

The Secure Systems group at IBM Watson works in two camps:

- As part of IBM Research, we are interested in basic research questions regarding what it *means* for a system to be secure, *how* to make systems secure, and *what* to do with them after that.
- However, in the past few years, we have had the chance (as part of a team with other parts of IBM) to move some of the ideas from the laboratory to the real world, as the IBM 4758 family of cryptographic coprocessors.

Our group has a unique perspective on FIPS 140-N. As part of the 4758 work, our group did the documentation, testing, and modeling that led to the 4758 earning the world's first FIPS 140-1 Level 4 validation (and, to date, the only device with software to reach this level). However, as "researchers," we cannot immerse ourselves in this depth of work without thinking about where it might be extended and improved.

We filed an earlier statement during the comment period before the 140-2 draft was released. Now, we offer these comments in particular to the 140-2 draft.

Positives

Before we launch into a litany of drawbacks, we want to stress: It is absolutely critical that secure systems be independently evaluated against a standardized metric, and FIPS 140-N remains the only suitable metric for tamper-resistant hardware and secure coprocessors. We support the standard.

Additionally, we were pleased by many of the changes in the 140 2 draft, including:

- the clarification of physical security requirements vs. module type;
- the clarification of when the OS requirements apply;
- the liberation of the OS requirements from the somewhat out-dated Orange Book functionality;
- the unification of software and hardware design assurance (since, if a module has both, the security architecture and analysis must address both—we lost some time in our 4758 validation due to incorrectly dividing labor along hardware vs. software lines); and
- the addressing of the overall life cycle of the module (since, the security of a module in practice depends on more than just the design of the module, but also on issues such as how it gets initialized and shipped).

Negatives

However, we have concerns about several areas where the 140-2 draft did not go far enough.

Hardware RNG Hardware sources of good random numbers exist, and some scientists would argue that "only the laws of physics can provide trustworthy randomness." We urge NIST to consider explicitly including hardware RNGs within the scope of 140-2.

Software Penetration Like 140-1, the draft 140-2 requires much rigorous *hardware* penetration testing at the higher levels—but does not require any comparable level of *software* penetration testing.

Many modules (such as the IBM 4758) include both hardware and software elements, where the internal software handles requests from outside. For many adversaries, the first line of attack will be via these requests.

- Can malformed requests or out-of-range parameters cause insecure behavior?
- Is the internal module software subject to any buffer overflow problems?

As part of our 4758 submission, we included explicit analysis of these issues, because it was the right thing to do, and because we hoped to set a precedent for future Level 4 validations. We urge NIST to, minimally, require such analysis for all higher-level modules that have software elements (particularly when the OS requirements do not otherwise apply).

(In Appendix B, the draft standard optionally recommends using assertion statements to do range checking on parameter. While this is a good start, we still recommend *mandatory* tests or documented countermeasures for out-of-range parameters, but permitting the vendor to use whatever techniques—not necessarily assertion statements—are approriate.)

"State" Terminology As we noted in our earlier comments, the use of the term "state" in the software FSM requirements, as practiced, leads to continual misunderstandings with our colleagues in the academic software verification community.

- In the research world, "state" is a possible condition of the system (e.g., a huge tuple describing every relevant parameter). Execution of a portion of code transforms the state of the system; thus, the complexity of a particular verification exercise is measured by the number of states of the system.
- However, in the FIPS 140-N world, "state" is the chunk of code—e.g., the transformation function. We need to invent another term for the "condition of the system" that gets transformed.

As a consequence of this unfortunate terminology, it takes much careful conversation for the cutting-edge academic researchers to understand what the FIPS 140-N process involves.

Minimally, we urge NIST to explicitly clarify this terminology in 140-2. (Ideally, it would be nice for 140-2 to use the same terminology that academic researchers do.)

EAL Levels for OS We were happy to see the change from Orange Book to Common Criteria—both because (as noted earlier) the latter allows more flexible functionality, as well as because unifying FIPS 140-N requirements with international standards where appropriate will make it easier for vendors to cross-validate products.

However, we noticed with concern that the Common Criteria *assurance* levels called out in the draft 140-2 are one level weaker than the Orange Book levels called out in 140-1.

Unlike the Orange Book, the Common Criteria describes systems using two orthogonal parameters:

- the functionality level, and
- the assurance level.

Standards such as the Orange Book use one parameter.

The Common Criteria EAL levels only specify the level of *assurance*, and not the level of functionality. The assurance mappings between the TCSEC, the European ITSEC, and the Common Criteria work as follows:

TCSEC	ITSEC	Common Criteria
A1	E6	EAL7
B3	E5	EAL6
B2	E4	EAL5
B1	E3	EAL4
C2	E2	EAL3
C1	E1	EAL2
—	—	EAL1
D	—	—

To achieve a comparable level of assurance under the Common Criteria to match a TCSEC B2, then FIPS 140-2 should specify EAL5. Functionality requirements are specified separately from the assurance requirements, and it might be valuable to develop a Common Criteria protection profile for the crypto devices that FIPS 140 is trying to cover.

Additional Levels We reiterate our previous statements regarding the need for an additional hardware level in 140-2. From a hardware perspective, going from a minimal Level 3 module to a Level 4 module can lead to a huge increase in the difficulty of manufacturing. But it is possible and reasonable to to build a significantly more secure Level 3 module without this increased difficulty. We recommend that NIST consider an explicit Level 3.5 that acknowledges this intermediate level of security. (and cite our earlier comments for a possible spec).

On the other hand, we also have concerns that the software requirements of even Level 4 do not go far enough to describe emerging high-assurance work. There are some devices out there that are applying a *higher* level of assurance than TCSEC B2 or Common Criteria EAL5. The best example is the Multos Smart Card operating system that has now received an E6 certificate under the ITSEC scheme in the UK. Another example is the smart card operating system project that we are working on at IBM that is also aiming at higher than EAL5. Our concern is that FIPS 140-2 does not provide any means for recognizing those additional levels of software assurance. Given the existence of Multos as a commercial product with an E6 certification from the UK, perhaps it is time for FIPS 140-2 to have levels higher than 4. One thought would be that an EAL6 might give FIPS 140-2 Level 5, and EAL7 might give FIPS 140-2 Level 6. (But note that this is a not a fully developed proposal; in particular, we haven't thought about what hardware assurance one would want for Levels 5 or 6)

U.S. Government Standards

Microsoft Comments

FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0398

TABLE OF CONTENTS

OPENING

Microsoft understands the importance of the NIST Cryptographic Module Validation Program and is pleased to provide comments and questions regarding the NIST FIPS 140-2 draft at http://csrc.nist.gov/cryptval/140-1/fr991117.htm.

If NIST is interested in establishing a dialog with Microsoft to discuss these comments and questions, please send email to: patar@microsoft.com;tiffanyj@microsoft.com;fedprp@microsoft.com

COMMENTS

1.2 Security Level 2

Operating system security requirements should be applicable for all cryptographic modules relying on an hosting operating system to provide communication paths between an authorized user and the cryptographic module.

The FIPS 140-2 draft states “a trusted operating system is needed in order for software cryptography to be implemented with a level of trust comparable to hardware cryptography”.

We acknowledge the specific operating system security requirements are listed in Section 4.6. These include the CAPP requirements and a list of events that require auditing.

While some auditing events are aimed to counter specific threats only when a software cryptographic module is used in a hosting operating system, there are other auditing events that also counter threats in the case where a hosting operating system is required to provide communication paths between an authorized user and a hardware cryptographic module such as smart card or PC card. Microsoft recommends the events (bulleted below) be recorded for all cryptographic modules requiring a host operating system to provide communication paths between an authorized user and the cryptographic module, to achieve FIPS-140-2 Level 2 or higher:

- Attempts to provide invalid input for cryptographic officer functions [associated with the cryptographic module],
- The addition or deletion of a user to/from a cryptographic officer role [associated with the cryptographic module] (this is valid at least in the case the cryptographic module is a smart card or PC card),
- All requests to use authentication data management mechanisms [associated with the cryptographic module],
- Use of a security-relevant cryptographic officer function [associated with the cryptographic module],
- All requests to access user authentication data [associated with the cryptographic module],
- All use of an authentication mechanism (e.g. logon) [associated with the cryptographic module],
- All attempts to use the user identification mechanism, including the user identity provided [and associated with the cryptographic module],
- Explicit requests to assume a cryptographic officer role [associated with the cryptographic module],

- The Allocation of a function to a cryptographic officer role [associated with the cryptographic module].

The Level 2 requirements to audit the above events should not be applicable to only software cryptographic modules, but all modules that require a hosting operating system to provide communication paths between an authorized user and the cryptographic module. This is consistent with the NIST "Security Requirements for Certificate Issuing and Management Components". Regardless of whether a cryptographic module is hardware or software, operating system auditing requirements for the events outlined above are needed by NIST "Security Requirements for Certificate Issuing and Management Components". Additionally, the security issues associated with the hosting operating system used by a smart card cryptographic module are discussed in Secure Applications for Handheld Devices: http://www.cs.princeton.edu/sip/projects/handheld/. In other words, a cryptographic module, requiring a hosting operating system to provide communication paths between an authorized user and the cryptographic module, should not be able to achieve Level 2 security if the hosting operating system is not able to audit the events (bulleted list above) in a secure manner (i.e. protected with the rest of CAPP functionality).

The requirement to audit the execution of the tests of the underlying machine and the results of the tests is not consistent with the CAPP requirement

The tests refer to the Abstract Machine Testing (FPT_AMT.1.1) defined in the CAPP as follows:

> 5.5.1.1 The TSF shall run a suite of tests [selection: during initial start-up, periodically during normal operation, or at the request of an authorized administrator] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
> Application Note: In general this component refers to the proper operation of the hardware platform on which a TOE is running. The test suite needs to cover only aspects of the hardware on which the TSF relies to implement required functions, including domain separation. If a failure of some aspect of the hardware would not result in the TSF compromising the functions it performs, then testing of that aspect is not required.
> Rationale: This component supports the O.ENFORCEMENT objective by demonstrating that the underlying mechanisms are working as expected.

In most commercial operating systems, these tests do not run automatically but are run manually by an operator. Also, these tests need not be a part of the operating system. In these operational scenarios, the auditing requirement specified in Section 4.6 of FIPS-140-2 may not be necessary.

1.2 Security Level 3

Reference: “show status via a trusted mechanism” requirement. This should not be applicable to only software cryptographic modules.

This requirement should be applicable to smart card or PC card cryptographic module that does not use a card reader that has a “show status” interface.

QUESTIONS

1. Within Windows 2000, role separation provides the ability for system administrators to set the policies for the management functions including auditing. The operating system would provide role separation between a domain user and domain administrator (user and cryptographic officer roles respectively). Would the role requirements for maintenance mode be required if the cryptographic module doesn't provide for the notion of maintenance? Would operating system management of roles be sufficient?

2. For FIPS 140-1, one of the areas confusing to us was that of the FIPS 140-1 required cryptographic algorithms and those used by various protocols like SSL3 and TLS. Both the SSL3 and the TLS protocols use MD5 and SHA when performing key derivation. The method used by TLS is considerably better than the one used by SSL3 so we believe this should be acceptable to NIST. Is it possible to gain insight and official NIST consensus from a FIPS 140-x perspective on the following IETF TLS cipher suites?

    a. TLS_RSA_WITH_DES_CBC_SHA

    b. TLS_RSA_WITH_3DES_EDE_CBC_SHA

    c. TLS_DH_DSS_WITH_DES_CBC_SHA

    d. TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA

3. Similarly, we believe NIST should be involved in more than just the certification of cryptographic modules. We believe industry and the federal government would appreciate guidance on which protocols are "FIPS compliant" (NIST approved). In addition we would like to know which exact algorithms may be used in these protocols. For example:

    a. SMIME v3 with DSS, DH and 3DES (or DES)

    b. TLS with RSA, SHA-1 and 3DES cipher suite

    Without this information government agencies are still going to make purchases of cryptographic products, which may use a certified cryptographic module but may not be using it with protocols that are "approved". The cryptographic module validation is a piece of the framework but at this point there is no official position on protocols. We believe both the module and the protocols play important roles in the security of cryptographic products. Just as NIST publishes FIPS for approved algorithms, we believe NIST should consider publishing FIPS for approved protocols.

4. A cryptographic module must be able to return a current status of the module and must be able to initiate a self-test on demand. There is no guidance on how a software module might do this or if software is exempt from this hardware-centric requirement. Would NIST please clarify?

From: "Knowles, Neil, Mr, AFCIC/SYIP" <Neil.Knowles@pentagon.af.mil>
To: "'Proposed140-2@nist.gov.'" <Proposed140-2@nist.gov>
Subject: United States Air Force Inputs to Proposed FIPS 140-2
Date: Tue, 15 Feb 2000 15:32:46 -0500
Importance: low
X-Mailer: Internet Mail Service (5.5.2650.10)

We have reviewed subject document, circulated it among applicable offices, and have no comments at this time.

GENERAL DISA COMMENTS ON DRAFT FIPS 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

1. The Defense Information Systems Agency (DISA) has reviewed the draft FIPS, and recommends that it not be issued until major modifications have been made to address: (1) the information assurance (IA) environments to which the FIPS applies, and (2) the application of the FIPS to both FIPS-approved and non-FIPS-approved cryptographic algorithms. Also, the FIPS coordination process needs to be fixed so that the Federal agencies, who are supposedly bound by FIPSs, have at least as much time to review FIPS coordination drafts as the public, who are not bound by FIPs.

2. The "X.509 Certificate Policy for the United States Department of Defense" categorizes information systems according to (1) the value of the information in them, (2) the threats to them, (3) the level of environmental protection afforded to them. These three factors determine the assurance level of a public key certificate used to protect or authenticate information; and this assurance level, in turn, determines the critical technical and operational parameters of a public key infrastructure. The FIPS recognizes the need to define different cryptographic module security levels for different IA environments, but the FIPS never satisfies this need, as it never actually defines the IA environments and their associated cryptographic module security levels. DISA recommends that NIST consider DOD's X.509 certificate policy as an example of how to specify security requirements for low, medium, and high value unclassified information in minimal, moderate, and high protection environments.

3. The security of a cryptographic module depends primarily on: (1) the mathematical properties of the algorithms it implements, (2) the implementation of the module in hardware, software, or firmware, and (3) the administration of the module (maintenance, manual keying, etc.). The need to protect Internet electronic commerce has spurred development and deployment of non-FIPS-approved, commercial algorithms with good mathematical properties. However, commercial standards do not adequately specify the implementation and administration of these algorithms, and FIPS 140-2 can fill these gaps in commercial standards.

It is important that the Federal Government exploit commercial algorithms to support cost-effective cryptographic interoperability with its citizens, suppliers, and allies. Therefore FIPS 140-2 must not require FIPS-approved algorithms, because not all such algorithms are commercially supported. FIPS 140-2 should specify implementation and administration requirements for both FIPS and non-FIPS algorithms.

4. Draft FIPS 140-2 was released to the public for formal comment on 17 Nov 1999, but was not sent to the Federal Agencies for formal comment until 11 January 2000. Furthermore, it was not sent the DOD Senior Management Official for FIPS, Mr. Jerry Smith, who works for the DISA Joint Information Engineering Organization's Center for Information Technology Standards. Mr. Smith has not seen any FIPSs for formal coordination in at least two years. Apparently, the FIPS coordination process has changed and DISA has not been informed of the change. DISA requests that NIST publish its procedures for FIPS coordination.

5. Specific comments follow. DISA Point of contact is Mr. Leonard Swatski, Code JEBA, (703) 735-3233.

SPECIFIC DISA COMMENTS ON DRAFT FIPS 140-2

1. Page ii, Paragraph 7. It is not clear whether the FIPS applies to classified information. This paragraph should state whether the FIPS applies to classified information, and if so, the classification level to which it applies.

2. Page ii, paragraph 11, first sentence. Change "shall" to "may".

Rationale: If FIPS 140-2 mandates FIPS-approved algorithms, then Federal agencies will not be able to exploit many commercial products to protect sensitive, unclassified information. While NIST has been successful in getting many FIPS-approved algorithms adopted by commercial standards bodies, many popular commercial algorithms are not included in FIPSs. Non-FIPS-approved algorithms should be included as part of NIST's Cryptographic Module Validation Program. Examples of such algorithms are:

Symmetric Key	Hash	Public Key	Key Dist.
RC4	MD5	PKCS#1 (RSA)	RSA
RC5		ECDSA	X9.42
IDEA			
Blowfish			

3. Page iv, Paragraph 15. Five years is too long to wait to review this standard. We recommend that the standard, and its associated implementation guidance, be reviewed every two years.

4. Page 1, paragraph 1, second subparagraph. This paragraph recognizes that security levels for cryptographic modules are determined by the value of information and the protection environment. However, the FIPS does not define information value levels and protection levels. Information value levels and protection levels should be defined, and examples included, as in the "X.509 Certificate Policy for the United States Department of Defense", Version 5.0, 13 December 1999.

5. Page 2, paragraph 1.2, third subparagraph. This subparagraph specifies requirements for security level 2 software cryptography for multi-user timeshared systems.
Do these requirements apply to client-server networks as well?
Similar comments apply to paragraphs 1.3 and 1.4.
Also, "EAL2" needs to be defined as "Evaluation Assurance Level 2".

6. Page 4, Paragraph 2.1, "Approved security function". This broad, almost circular definition defines "approved security function as a cryptographic algorithm or technique, an authentication technique (which may be password-based), or evaluation criteria specified or adopted in a FIPS. Under this definition, a cryptographic module implementing password-based authentication in accordance with FIPS 112, or being certified at Common Criteria Evaluation Assurance Level 2, could be considered as functioning in an Approved mode of operation.
This weakens the definition of "Approved mode of operation".
Furthermore, paragraph 4.1, first subparagraph, implies that Approved algorithms and Approved security functions are different things, when in fact Approved algorithms are a subset of Approved security functions. We recommend that this definition be replaced with a definition of "approved algorithm", and that separate definitions of "authentication technique" and "evaluation criteria", be created, if necessary.

Also, the current definition states that "Approved Security functions are listed in the Implementation Guidance for this Standard". However, no such Implementation Guidance document exists for draft FIPS 140-2, but does exist for FIPS 140-1. Such implementation guidance is critical to this standard, as it is the only source of approved algorithms. NIST must produce such implementation guidance before this FIPS is approved.

7. Page 12, paragraph 4.1, first subparagraph, second sentence. Change "shall" to "may". The rationale is the same as for detailed comment #2 above.

8. Page 21, paragraph 4.5.2. The phrase "high probability" needs to be replaced with a numeric value.
This comment also applies to other instances of this phrase in the document.

9. Page 22, paragraph 4.5.3., top two sentences. The phrase "pick-resistant mechanical locks", should be better defined and

should include some measure of the time needed to break the lock.

10. Page ii, paragraph 7, "Cross Index", and pages 49-50, "Selected Bibliography". FIPS 113, "Computer Data Authentication", and FIPS 171, "Key Management Using ANSI X9.17", are listed on these pages, but are not referenced in the body of the standard. Furthermore, we understand that NIST is no longer validating products to these standards. If this is the case, why are these standards referenced?

From: Craig Ogg <cogg@stamps.com>
To: Proposed140-2@nist.gov
Subject: FIPS 140-2 Draft Comments
Date: Tue, 15 Feb 2000 22:31:38 -0800
X-Mailer: Internet Mail Service (5.5.2650.21)

Software Development Practices
Methods to modify code flow and/or execute untrusted code are a common vector of attack and as such, we propose that "best practice" software development practices that increase the security of a cryptomodule be adopted as requirements in the standard. Specifically, many of the techniques described in Appendix B of FIPS 140-1 will go a long way towards mitigating such attacks. At a minimum, protection against buffer overrun attacks should be mandated.

Data Authentication
HMAC (per RFC 2104) has already been accepted for entity authentication and its use should be permitted for data authentication. Requiring DES MAC (FIPS 113) for this usage can lower the effective security of a cryptomodule.

Non-Key/Authentication Related CSPs
A cryptomodule may be called upon to cryptographically protect value-based processes within its boundary. For example, a postage meter's primary goal is to cryptographically protect the integrity of its financial data. The FIPS should include such data elements and provide guidelines to ensure that they are manipulated and accessed in a secure fashion.

Guidance Documentation
Under FIPS 140-1 a vendor can create a separate, non-proprietary version of the cryptomodule's Security Policy for public distribution. The Guidance Documentation added in 140-2 appears to be designed to also be distributed publicly. If this is the case, we strongly recommend that a separate non-proprietary version also be allowed for the Guidance Documentation. NIST should not require vendors to distribute proprietary information publicly in order to receive validation.

Craig Ogg
Chief Technologist
Stamps.com
3420 Ocean Park Blvd. Suite 1040
Santa Monica, CA 90405

Mr. Ed Roback, Acting Chief
Computer Security Division
National Institute of Standards
  and Technology
Building 820, Room 426
Gaithersburg, Maryland 20899

Dear Mr. Roback:

Reference your email dated January 11, 2000, that you sent to Federal Chief Information Officers, requesting comments on Draft Federal Information Processing Standard (FIPS) 140-2. This office, along with some other offices within the Department of Energy, reviewed this draft standard and developed a number of comments. The comments were compiled and are listed on the attachment.

Our comments are from the viewpoint of a user of cryptographic modules and the FIPS. The definition of "user" in this case is one who will use FIPS 140-2, and other government requirements documents, to design and build information management systems that process sensitive unclassified information. In addition, FIPS 140-2 and other government requirements documents are used to evaluate and determine the suitability of vendor products for specific applications.

We are submitting our comments electronically, as suggested in your email. In addition, a hard copy will be mailed to your office.

Thank you for the opportunity to review this draft standard. Should you have any questions regarding our comments, please call Sharon Shank on (301) 903-3047.

Sincerely,

John M. Gilligan
Chief Information Officer

Attachment

COMMENTS TO FIPS 140-2

1. FIPS 140-2 is a very complex document in itself, and it is made even more intractable by referencing documents like the Common Criteria. Part of the apparent complexity is due to the intent of grouping together the requirements for cryptographic modules in many different form factors for many different applications. The attempt is admirable but the net result is confusion. We suggest that, as a minimum, there should be segmentation of software and hardware module requirements. It may also be useful to have a section on devices normally referred to as cryptographic tokens, keys, or smart cards as these devices seem to be part hardware and part software.

2. We think the term used to specify the various levels of modules, Security Level l, Security Level 2, etc., is misinterpreted by some people. They assume that using a Security Level 4 cryptographic module means they have a "Security Level 4 system". Conversely, they assume that a Security Level 4 module is required for a "high security system". The overall security level of an information management system is a function of many components and security disciplines. Perhaps the title should be changed to "Requirements for Cryptographic Modules" and the various levels be identified as Level 1, Level 2, etc., rather than "Security Level 1".

3. Page ii, Part 11, last paragraph: The sentence "If a cryptographic module is required to incorporate a trusted operating system, then the module shall employ trusted operating systems that have been evaluated by an accredited evaluation authority" is confusing. Is this sentence addressing a single or multiple chip hardware module, or a software module? If referring to a hardware module, does this mean the modules' internal operating system or the operating system of the computer to which it may be connected? If addressing a software module, is this referring to the computer operating system? We are under the impression that if an operating system is "trusted", then an accredited authority has evaluated it. Or does this sentence imply that the operating system in question is "trust for the intended application"?

4. Page iii, Part 15, second paragraph, and Page 1, Part 1, paragraph 3: "While the security requirements specified in this standard are intended to maintain the security of a cryptographic module, conformance to this standard does not guarantee that a particular module is secure. It is the responsibility of the manufacturer of a cryptographic module to build the module in a secure manner." This paragraph seems to negate the intent of the entire document and process. Paraphrased, it says two things: 1) the standard is no good, and 2) there is no requirement for the manufacturer to build and deliver the module that was tested.

5. The last paragraph of Section 1. states "Cryptographic modules, incorporated into commercially available products, have been validated to meet every security level specified by this standard." Since the standard has not been finalized, it does not seem possible for any modules to have been validated to it. We think this means that the products have been validated to equivalent requirements in FIPS 140-1.

6. Page 1, Section 1.1, paragraph 2: The sentence "Such implementations may be appropriate for low-level security applications.", is misleading in that a Level 1 software cryptographic

module may be quite useful in some high-security information systems when other issues, such as overall system physical security, computer security, network security, and personnel security, are taken into consideration. A statement such as "Such implementations may be appropriate for some information security system applications.", may be less misleading.

7. Page 2, Section 1.2, third paragraph: In the sentence, "Security Level 2 also allows software cryptography in multi-user timeshared systems . . .", we are not sure what is meant by "multi-user timeshared systems".

8. Page 10, Part 3: Functional Security Objectives. The first item on the cryptographic module objectives list should be to correctly implement the cryptographic algorithms that are contained in the module. There should also be an objective to ensure proper operation, or at least change to a "fail-safe mode", when the module is not operated in an Approved mode.

9. Section 4.1 states "A cryptographic module shall implement at least one Approved algorithm or Approved security function used in an Approved mode of operation." Is there a need for modules that only implement algorithms or security functions, but not both?

10. Page 24, Section 4.6, Operating System Security, it is not clear if the operating system referenced in this section is the computer OS or cryptographic module OS.

11. Section 4.7.2 states "Internal key generation is optional." We suggest that internal key generation should be mandatory for all modules that perform digital signatures with the possible exception of security level 1. Most Certificate Policies require FIPS 140-1 level 2 or higher hardware cryptographic modules for Registration Authorities (and other users depending on assurance level), and that they generate the key pair in the module. To have non-repudiation of digital signatures at other than a rudimentary level of assurance, it is commonly considered necessary to have the key pair generated in the users' cryptographic module so that it is always under their control.

12. We would like to see a section or an appendix that crosswalks the FIPS 140-1 levels to the FIPS 140-2 levels and highlights any differences. This would be helpful since many Certificate Policies require FIPS 140-1 validated cryptographic modules at specific levels.

13. We would like to see a reference to a list of Common Criteria validated commercial operating systems (e.g., Novel 4.11 is EALn), and a crosswalk of the CC evaluation assurance levels to the National Security Agency ratings.

14. We would prefer to be able to obtain more information about the product, as evaluated, from the Validated Products List. Since one of the significant changes from FIPS 140-1 to 140-2 seems to be the addition of reference to the Common Criteria, it would be good for the Validated Products List to reference which components of the CC were invoked in testing of a crypto-module.

Date: Wed, 16 Feb 2000 08:08:03 -0500
From: brianes1 <brianes1@ucia.gov>
X-Mailer: Mozilla 4.61 [en] (WinNT; U)
X-Accept-Language: en
To: Proposed140-2@nist.gov, dougljn1@ucia.gov, sherrln@ucia.gov
Subject: CIA Comments on Proposed FIPS140-1

Below please find CIA's specific comments on the draft FIPS140-2 on cryptographic modules security requirements. If you have anyquestions regarding these comments, please contact Ms. Sherrill Nicely, CIA CIO Staff, at sherrln@ucia.gov.

Regards,

Brian Sowers
Executive Officer
CIO Staff

1. Announcement section, page iii, paragraph 14: one year after this new standard is approved we must buy only FIPS 140-2 crypto modules. It's not clear that commercial vendors will be able to providecertified modules within that time.

2. Announcement section, page iv, paragraph 16: provides requirements for Agency heads to issue waivers to the requirement to purchase only FIPS 140-2 certified crypto modules. The waiver process requires the submission of detailed information that may be objectionable from an operations security perspective. This paragraph also states that information on procurement waivers must be published in the CBD--something we do not do as normal practice.

3. Section 1, pages 1-3: Security Levels 3 and 4 are described as being able to be implemented either by hardware of software. However, in the rest of the document, there is a strong implication that Security Level 4 requires hardware. (for instance, Section 5 refers to tamper detection and environmental failure protection and testing for Security level 4: physical parameters specific to hardware--what about software?)

4. Section 4, pages 11-37: it needs to state whether or not it is assumed that knowledge of the encryption algorithm has a bearing on the security of the system. Are they requiring that in Level 3 and 4 that the system needs to hide what algorithm is being used? This is mentioned in the Power Analysis para on page 37, but is vague and not clearly stated. Also, suggest that if a certain hardware cryptographic module is used to provide Level 4 security, that there be something in this document that prevents it being used in a Level 1, 2, or 3 product.

5. Section 4.2, page 13, paragraph 1: recommend changing the last sentence to: "An Application Program Interface (API) of a software component of a cryptographic module may constitute a logical interface for some security levels."

6. Section 4.3.3, page 15: Recommend amending the first bullet to read: "For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g. guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods.) In addition, each authentication attempe must take at least N seconds."

7. Section 4.4, page 17, bypass states are not a good idea--especially in Level 4. Would also like to see a specification for tamper coatings and seals.

8. Section 4.5.5, page 23, Environmental Failure Protection Features: Why just temperature and voltage? What about RF, H-field? Also, suggest adding some kind of specification for the detection of input and output data to the cryptographic module that is out of bound of what is expected during normal operations.

9. Section 4.6, pages 24-27: states that in the case of a product that uses cryptographic software as well as untrusted user supplied software, then the "hardware, operating system, and cryptographic software are considered part of the cryptographic module." What about the untrusted user-supplied software? This leaves the system open to a virus attack or a trojan horse attack. While the operating system is addressed, what about the BIOS on the host system?

10. Section 4.7, pages 27-29: The paragraph clearly states how keys will be stored inside the module, but does not requre any controls on key dissemination or storage outside the module--for example, if the keys are entered via a keyboard, or from a downloaded file, there should be a provision that temporary files will not be retained by the computer. Recommend some statement about key zeroization that requires that all possible storage locations of keys be earase and/or overwritten.

11. Section 4.9, pages 30-32: There is no mention of periodic run-time tests performed by the cryptographic module while in operation to verify that it is functioning properly. Also, recommend that a statement that all self-test be executed within the boundaries of the cryptographic module.

12. Section 4.10.1, page 33: For Level 1, each item is to be labeled with a unique id number. If this isn't tracked, why do this?

13. Section 4.10.4, page 36: Suggest that they require than an 'application-specific' policy document describing what to do if the other guidance documentation is not followed be written and enforced in order for a system to be FIPS 140-2 compliant.

From: NSFCIO <NSFCIO@nsf.gov>
To: "\"'<Proposed140-2@nist.gov>'\" <"<Proposed140-2@nist.gov>
Subject: comments on draft Federal Information processing
Date: Wed, 16 Feb 2000 17:25:15 -0500
X-Mailer: Internet Mail Service (5.5.2650.21)

The National Science Foundation has no comments on the proposed revision.

Linda P. Massaro
Chief Information Officer
National Science Foundation

From: James.Downes@cio.treas.gov
Subject: OTAR Requirement
To: proposed140-2@nist.gov
Cc: "Austin, James" <JAustin@tiscom.uscg.mil>, billp@its.bldrdoc.gov,
fbi09@earthlink.net, Dwight.Locke@cio.treas.gov, jfoti@nist.gov,
Tom.Wiesner@cio.treas.gov
Date: Fri, 18 Feb 2000 12:45:45 GMT
X-MIMETrack: Serialize by Router on CIOMAIL/CIO/TREAS/GOV(Release 5.0a |May 4, 1999) at
02/18/2000 07:46:04 AM

The attached memo is provided on behalf of the INFOSEC Working Group of the Federal law Enforcement Wireless Users Group (FLEWUG) who are major users of encryption in their wireless systems.

If you have any questions contact me at (202) 622-1582 or via e-mail. We thank you in advance for your consideration in this matter.

(See attached file: Draft NIST Memo_FIPS140-2.doc)

Jim Downes

TO: Proposed 140-2@nist.gov

CC: FLEWUG INFOSEC Subcommittee

SUBJECT: Requirement for OTAR

In reviewing th eproposed FIPS 140-2 document, an oversight has been noted in the area of Cryptographic Key Management (Section 4.7 in the document).

A number of users of the subject standards within the Federal Law Enforcement Wireless Users Group (FLEWUG) have requirements in the wireless communications systems they deploy for Over-The-Air-Rekeying (OTAR) of the subscriber devices. There seems to be no reference in this section of the document that addresses wireless rekeying of the subscriber devices. It appears that the only areas that are addressed are the manual connection of a key-fill device or a wireline connection for key-fill.

As stated previously, the FLEWUG member agencies are users of wireless equipment and use the standardized encryption algorithms to satisfy their particular operational needs. The ability to use OTAR is essential to the successful completion of these missions. Therefore, we feel strongly that OTAR is a requirement that must be addressed in the FIPS 140-2 document.

I thank you in advance for your consideration in this matter. If you have any questions or wish to discuss this matter further, feel free to contact me at (202) 622-1582 or via e-mail.

James Downes
Chair, FLEWUG INFOSEC Subcommittee
Department of the Treasury
CSM/WPO, Room 2150
1425 New York Avenue, N.W.
Washington, DC 20220